2022-12-11 Какими качествами должно обладать хорошее руководство аварийного восстановления?

Данный документ регламентирует порядок действий которые должен предпринять персонал в процессе возникновения проблемы для снижения последствий в краткосрочной перспективе и возможно включать в себя план по восстановлению целевого состояния системы.

Процесс восстановления в случае аварии должен опираться на используемые в текущем решении технологии обеспечения отказоустойчивости и высокой доступности. Например если речь идет о дисковой подсистеме то в состав данных технологий будут входить:

- RAID массив для защиты от выхода из строя дисков;
- Дублирование основных компонентов, отвечающих за предоставление доступа к данным;
- Дублирование каналов связи до клиента;
- Мгновенные снимки для защиты от изменений;
- Удаленная репликация для защиты от аппаратного сбоя;
- Резервирование площадки путем создания метрокластера;

За счет описанных выше технологий достигается достаточно высокий уровень надёжности подсистемы в целом, например производитель систем хранения данных уровня HiEnd - Hitachi Vantara заявляет что СХД VSP способны обеспечить 100% доступность данных (при построении территориально распределенных решений), а большинство производителей СХД среднего уровня прогнозирует отказоустойчивость своих систем на уровне “пять девяток”

Доступность %	**Время простоя в год**	**Время простоя в месяц**	**Время простоя в неделю**
90% (“одна девятка”)	36.5 дней	72 часов	16.8 часов
95%	18.25 дней	36 часов	8.4 часов
98%	7.30 дней	14.4 часов	3.36 часов
99% (“две девятки”)	3.65 дней	7.20 часов	1.68 часов
99.5%	1.83 дней	3.60 часов	50.4 минут
99.8%	17.52 часов	86.23 минут	20.16 минут
99.9% (“три девятки”)	8.76 часов	43.2 минут	10.1 минут
99.95%	4.38 часов	21.56 минут	5.04 минут
99.99% (“четыре девятки”)	52.56 минут	4.32 минут	1.01 минут
99.999% (“пять девяток”)	5.26 минут	25.9 секунд	6.05 секунд
99.9999% (“шесть девяток”)	31.5 секунд	2.59 секунд	0.605 секунд

Если мы касаемся технологий восстановления в случае аварии на площадке с учетом потери площадки целиком то приблизительное время восстановления напрямую зависит от применяемых технологий и уровня автоматизации.

1. Метрокластер - минуты;
2. Кластер с ручным переключением (напр. VMware SRM) - часы;
3. Репликация данных без кластера - дни;

Руководство аварийного восстановления должно в первую очередь служить цели регламентирования действий в случае обнаружения аварии и первичном реагировании для скорейшего восстановления работоспособности системы и строиться на базе используемых в проекте технологий обеспечения высокой доступности. С целью составления такого плана необходимо составить список технологий, которые обеспечивают высокую доступность и по каждой из них подготовить план действий в случае обнаружения аварии. Вторым методом можно предложить подход, основанный на анализе рисков. Необходимо составить перечень возможных аварийных ситуаций которые могут произойти с проектируемой системой и по каждой из них подготовить план действий по снижению последствий т.е. план реагирования. Стоит ли готовить планы реагирования на безвыходные ситуации, например выход единственной площадки из строя - вопрос открытый.

Качественное руководство должно включать в себя не только описание действий в момент аварии но и список операций для восстановления системы в исходное состояние. Например если мы говорим о репликации на уровне дискового массива - в списке действий во время аварии будут:

1. Приостановка репликационной пары;
2. Включение доступа на запись для slave тома;
3. Монтирование slave тома в ОС;
4. Запуск систем;

После устранения последствий аварии и в данном примере после восстановления исходной системы хранения важно выполнить все операции в нужном порядке. Например если просто включить репликацию - система которая была главной до сбоя уничтожит все наработанные данные на резервной площадке. Поэтому например план восстановления в исходное состояние будет включать:

1. Разворот репликационной пары;
2. Ожидание полной синхронизации изменений на основную площадку;
3. Начало окна простоя;
4. Остановка сервисов на резервной площадке;
5. Разворот репликационной пары в оригинальном направлении;
6. Запуск сервисов на основной плоащке;
7. Конец окна простоя.

Последовательность действий по восстановлению к исходному состоянию является не менее важной процедурой в плане аварийного восстановления и в отличие от плана аварийного реагирования на сбой должна присутствовать для каждого проектируемого сбоя.